APPENDIX III

TAB N

Federal Rule of Civil Procedure 26 Disclosure of Expert Testimony

Jeffrey Shallit, Ph.D.

May 5, 2005

Case: Tammy Kitzmiller, et al. v. Dover Area School District and Dover Area School District Board of Directors
Case No. 04-CV-2688

I am a mathematician, computer scientist, and professor in the School of Computer Science at the University of Waterloo in Waterloo, Ontario. The School of Computer Science is one of Canada's most renowned academic departments, with approximately 60 faculty members. As my *curriculum vitae* describes in more detail, I have published approximately 80 papers in mathematics, computer science, and other areas, as well as co-authored two published books. My research has been funded both by the US National Science Foundation (NSF) and Canada's Natural Science and Engineering Research Council (NSERC).

In my lectures at the University of Waterloo I often cover the concepts of Kolmogorov complexity theory, and it forms a section in a new book I have written on formal language theory, which has recently been accepted for publication by Cambridge University Press.

I also have an interest in pseudoscience and pseudomathematics. I spent three months of my sabbatical during the academic year 2001–2002 analyzing Dembski's arguments in his book *No Free Lunch*. I later published my analysis of Dembski's mathematical arguments in (1) a peer-reviewed contribution to the journal *BioSystems* [16]; and (2) a chapter entitled "Playing Games with Probability: Dembski's Complex Specified Information" in a book published by Rutgers University Press, entitled *Why Intelligent Design Fails* [19]. This latter contribution was co authored with Wesley Elsberry. A longer version of our paper is under review [6]. Other contributions discussing intelligent design include a set of challenges to intelligent design advocates [5] (none answered so far) and an analysis of how Dembski misrepresented an exhibit at the Smithsonian [17].

In evaluating Dembski's arguments I think it is useful to see both why his arguments are wrong and why the claims about them are inflated. In particular, I think it is useful to understand why Dembski would not be viewed as "the Isaac Newton of information theory" (as claimed by intelligent design proponent Rob Koons) by mathematicians who actually work and publish papers in information theory. Along these lines I had already (in May 2004) published an analysis of Dembski's mathematical achievements [18].

I am not receiving any compensation for this contribution other than travel expenses.

1 Dembski is not a scientist

In the popular and (especially) religious press, William Dembski is often, and erroneously, described as a scientist. For example, in 2000 *Christianity Today* stated, "Baylor University in October terminated well-known Intelligent Design scientist William Dembski as head of the Michael Polanyi Center for Complexity, Information, and Design." [1] Dembski even describes himself this way, for example, by signing the Discovery Institute's statement, "A Scientific Dissent from Darwinism", which states "The following scientists dispute the first claim..." [4] Dembski's name appears prominently.

However, by any reasonable standard, Dembski is not a scientist. For example, he possesses no advanced degrees in any scientific field. His advanced degrees are in philosophy, theology, mathematics, and statistics.[1] Dembski does possess a 1981 B. A. in psychology, but does not appear to have published any scientific work in psychology.

Unlike genuine scientists, Dembski does not submit his claims to the scrutiny of his peers. He has not published a single paper in a scientific journal. To the contrary, he exhibits contempt for the process of peer-review: he has been quoted as saying "I've just gotten kind of blase about submitting things to journals where you often wait two years to get things into print," he says. "And I find I can actually get the turnaround faster by writing a book and getting the ideas expressed there. My books sell well. I get a royalty. And the material gets read more." [12]

Dembski is not currently funded by any major scientific granting agency, such as the National Science Foundation. (He did receive an NSF postdoctoral fellowship for mathematics from 1988-1991).

2 Dembski is not a renowned mathematician

One of Dembski's advanced degrees is in mathematics, and he often phrases his claims in mathematical terms. Intelligent design supporters often point to his supposed mastery of advanced mathematics. However, Dembski's published output in mathematics is extremely small. It is very unlikely that his meager output would merit tenure at any major university.

The principal review journal in mathematics is *Mathematical Reviews* and its online version, called MathSciNet. Both are projects of the American Mathematical Society, the largest mathematical research organization in the world. The description of MathSciNet states that it is "a comprehensive database covering the world's mathematical literature since 1940." To illustrate its comprehensiveness, approximately 70,000 new reviews are added each year.

A search of MathSciNet for Dembski's mathematical research work turns up exactly four publications. There are two papers: one called "Uniform probability" that was published in the *Journal of Theoretical Probability* in 1990, and a survey article called "Randomness by design" that appeared in the philosophical journal *Noûs* in 1991. Neither of these published papers offers any support for the claims of intelligent design. The other two works reviewed by *Mathematical Reviews* are his 1998 Cambridge University Press book *The Design Inference*,

[1] I do not consider mathematics to be science.

and his 2002 book *No Free Lunch*.

Dembski's own CV lists two other mathematical publications (a 1990 article in the *Journal of Statistical Computation and Simulation* that was not reviewed by *Mathematical Reviews*). This article also makes no mention of intelligent design. The second is a mathematical paper entitled "Random Predicate Logic I" that Dembski apparently wrote back in 1990. In 2002, it appeared in Dembski's own electronic journal *Progress in Complexity, Information, and Design* which does not adhere to the ordinary peer-review process.[2] Neither this paper nor, indeed, the journal itself, is reviewed by *Mathematical Reviews*; this is some indication that the journal is generally considered to be of little mathematical value. (By contrast, an electronic journal that I edit, the *Journal of Integer Sequences*, often has its papers reviewed by *Mathematical Reviews*.)

To understand how sparse Dembski's output is, the average research mathematician publishes something like 1-2 research papers *each year*. Mathematicians at small colleges typically publish less because they have more teaching duties, while those with postdoctoral positions or research positions typically publish more. Dembski received his Ph. D. in mathematics in 1988. By 2005, a typical university mathematician would have published something like 17-34 papers in the peer-reviewed mathematical literature; Dembski has published two. (I do not count the paper in *Noûs* since that journal is a philosophy journal and the paper has no original mathematical research in it.)

Of course, the number of published papers is not the only measure of mathematical output. A good researcher could publish a small number of papers with large impact. It is therefore worthwhile to see how often Dembski's papers have been cited in the mathematical and scientific literature.

I used the ISI Web of Science (previously called Science Citation Index) to see how often Dembski's work was cited. His 1991 *Noûs* article has been cited five times (once by ID proponent Francis Beckwith in the *Harvard Journal of Law and Public Policy* and four other citations, including one in *Paleobiology*, but no citations in mathematics journals). Dembski's 1990 *Journal of Theoretical Probability* article has been cited twice (once again by Beckwith and once by L. Olsen in the *Mathematical Proceedings of the Cambridge Philosophical Society*). Dembski's 1990 article in *Journal of Statistical Computation and Simulation* has been cited three times (once again by Beckwith, once by Eliot Sober, and once by Barbour – none in mathematics journals). Since important mathematical papers routinely receive dozens or even hundreds of citations, this suggests that Dembski's mathematical papers have had essentially no influence among practicing scientists or mathematicians.

Dembski is frequently touted as an expert on information theory; his colleague Rob Koons has called him "the Isaac Newton of information theory". But how many research papers has Dembski published on information theory? According to MathSciNet, none. (By contrast, Aaron D. Wyner, an expert in information theory who died in 1997, has 64 entries in MathSciNet stretching over 40 years, for an average of 1.6 entries per year.)

[2] The web page `http://www.iscid.org/pcid.php` for the journal states "Articles accepted to the journal must first be submitted to the ISCID archive. To be accepted into the archive, articles need to meet basic scholarly standards and be relevant to the study of complex systems. Once on the archive, **articles passed on by at least one ISCID fellow will be accepted for publication.** The journal will be published in electronic form only (there will be no print version)." (Emphasis mine)

In his evidence statement, page 31, Dembski mentions his work on evolutionary computation through a simulation known as "MESA" (monotonic evolutionary simulation algorithm). However, a 2005 search on Web of Science did not turn up a single citation of this work by others. Indeed, there do not seem to be any results at all arising from this project.

Dembski himself states in an interview in *Christianity Today* that he "became something of an expert in the study of randomness". But how many original research papers has Dembski published on randomness? According to MathSciNet, none (or one, if one counts the survey in the philosophy journal *Noûs*). By contrast, Avi Wigderson, a colleague of mine who really is an expert in randomness, has 103 entries in MathSciNet (of course, not all of those are specifically about randomness).

Dembski argues that his books represent original mathematical research. But mathematicians have been very uncomplimentary about his work. David Wolpert, one of the inventors of the "No Free Lunch" theorems that inspired the title of Dembski's 2002 book, wrote a very uncomplimentary review for Mathematical Reviews, saying that his work "is written in jello". Mathematician Jason Rosenhouse, writing in the journal *Evolution*, criticized Dembski for unrealistic assumptions, for making assertions without substantiation, and for bogus probability calculations [15]. I criticized many aspects of Dembski's mathematics in a review that appeared in the journal *BioSystems* [16], in a popularized article [19], and a longer research article [6].

The quality and reputation of a mathematician can also be judged by the number and size of grants received from agencies that support mathematics, such as the National Science Foundation. To the best of my knowledge, Dembski currently holds no grants from these agencies. (He did once hold a postdoctoral fellowship in mathematics from NSF.)

Dembski's evidence statement (p. 29) makes a big deal of the fact that his work has been cited by other mathematicians, but the only example he lists is a paper by Chiu. I have read this paper, and, contrary to Dembski's claims, the paper makes no use of Dembski's methodology. For example, while Chiu cites Dembski's book *The Design Inference*, he uses the term "complex specified information", a term which does not even appear in that book! Neither does Chiu make any use of specifications, rejections regions, or background knowledge in his paper, all of which are essential parts of Dembski's "design detection" method.

I contacted in Chiu in 2003 to ask about his reference to Dembski, and his reply was that he had cited Dembski "as a courtesy". Courtesy references are very uncommon in legitimate mathematical research and cannot represent validation of Dembski's claims. Chiu's paper itself has not even been reviewed in *Mathematical Reviews*, which is good evidence of its lack of impact. Perhaps it is also relevant that Chiu is a "fellow" of Dembski's own "International Society for Complexity, Information, and Design" (`http://www.iscid.org/fellows.php`).

Finally, another measure of mathematical quality is whether the mathematician presents his/her work at mathematical conferences, such as those sponsored by the American Mathematical Society. To my knowledge, Dembski has never presented his claims at these standard fora for mathematical results.

3 Dembski's work is extensively criticized in the literature, but he rarely responds

One of the characteristics of pseudoscientists is their unwillingness to forthrightly address critics of their work. In this characteristic (and others), Dembski places himself in the camp of pseudoscientists.

David Wolpert, for example, the co-discoverer of the "No Free Lunch" theorems that are the major theme of Dembski's 2002 book, criticized Dembski's work in a review in *Mathematical Reviews*. Wolpert wrote that Dembski's "arguments are fatally informal and imprecise" and said that his work is "written in Jello".

Mark Perkah addressed many of Dembski's arguments in his work, *Unintelligent Design*, but Dembski has never responded.

I have criticized many of Dembski's argument in my review in *BioSystems*, pointing out, among other things, that the centerpiece calculation of *No Free Lunch* is off by about 65 orders of magnitude. An error this large would normally merit an immediate public correction, but Dembski has never acknowledged this or my other criticisms.

Probably the most fundamental empirical results that Dembski has ignored are the work of artificial life researchers. These researchers routinely find examples of complex structures or behaviors evolving at random — something that Dembski claims is impossible.

For example, in a celebrated paper, MacArthur fellow Karl Sims showed that complex strategies for locomotion and fighting could evolve purely randomly in digital simulations [20].

4 Dembski's method for inferring design is neither accepted by the scientific community at large, nor useful to science

Dembski claims to have a mathematical method for inferring when events have been designed by an intelligent being. The claim was first put forth in his book *The Design Inference*, where he gave a complicated multistep procedure called the "Generic Chance Elimination Argument", or GCEA. Roughly speaking this argument attempts to rule out all competing hypotheses based on chance, regularity, or some combination of these. After all these competing hypotheses have been ruled out, design is concluded.

In the preface of *The Design Infererence*, Dembski claims that his work will be of interest to "forensic scientists, SETI researchers, insurance fraud investigators, debunkers of psychic phenomena, origins-of-life researchers, intellectual property attorneys, investigators of data falsification, cryptographers, parapsychology researchers, and programmers of (pseudo-)random number generators". On page 3 of his evidence statement, Dembski goes even further, claiming that "forensic science, cryptography, random number generation, archeology, and the search for extraterrestrial intelligence (SETI)" already employ his "specified complexity" as a sign of intelligence. This claim is simply false. In the 9 years since the publication of *The Design Infererice*, no worker in these fields has successfully applied Dembski's

methods in published work.

Wesley Elsberry and I have published a series of eight challenges [5] concerning the applicability of Dembski's methods, but neither Dembski nor any of his supporters have taken them up. Dembski's claims of applicability are grandiose and unsupported.

One reason why Dembski's work is not useful to people who want to infer design is his insistence that design can only be inferred through an *eliminative* procedure; design is what is *left over* once chance and regularity are accounted for. There is no acknowledgment or recognition that design itself could be a form of regularity mixed with chance. Neither does Dembski admit that frequently the goal is to choose between competing design hypotheses (as in, "Who committed this murder?") or between design and regularity hypotheses.

A good example of the latter case is the discovery of pulsars. Pulsars (rapidly pulsating extraterrestrial radio sources) were discovered by Jocelyn Bell in 1967. She observed a long series of pulses of period 1.337 seconds. In at least one case the signal was tracked for 30 consecutive minutes, which would represent approximately 1340 pulses.

Bell and her research team immediately considered the possibility of an intelligent source. (They originally named the signal LGM-1, where the initials stood for "little green men".) The original paper on pulsars states "The remarkable nature of these signals at first suggested an origin in terms of man-made transmissions which might arise from deep space probes, planetary radar, or the reflexion of terrestrial signals from the Moon" [9].

However, the hypothesis of intelligent agency was rejected for two reasons. First, parallax considerations ruled out a terrestrial origin. Second, additional signals were discovered originating from other directions. The widely separated origins of multiple signals decreased the probability of a single intelligent source, and multiple intelligent sources were regarded as implausible. In other words, hypotheses involving design were considered at the same time as non-design hypotheses, instead of the eliminative approach Dembski proposes.

This *actual* example from the scientific literature should be contrasted with Dembski's claims about the *fictional* example based on Carl Sagan's novel, *Contact*, on page 3 of his evidence statement. Contrary to Dembski's claim, SETI (Search for Extraterrestrial Intelligence) researchers do *not* attempt to detect signals containing prime numbers or anything similar; instead they search for "narrow-band signals", on the theory that if intelligent beings are like us they will use these signals to communicate.

Another reason why Dembski's methodology is not useful is that he requires the elimination of *all* chance hypotheses before design can be inferred. In practice, this means that his method is an extended argument from ignorance. If no natural explanation for an event is currently known, Dembski would infer design. If later a natural explanation is found, the original inferernce would be in error.

A good example is the occurrence of circular and polygonal patterns of stones and soil that occur in cold environments. These patterns are "specified" in Dembski's sense and improbable relative to a uniform distribution of stones. They therefore would exhibit "specified complexity" and trigger a design inference. However, recently a detailed physical model has been proposed for these patterns [10].

More recently Dembski seems to have modified or even abandoned his complicated Generic Chance Elimination argument. For example, the GCEA in *The Design Inference* has 10 steps, while that in *No Free Lunch* has only 8. In *No Free Lunch*, the "rejection

regions" must be of a certain form, while in *The Design Inference* rejection regions are not explicitly mentioned.

Even stranger is the cavalier approach Dembski takes towards his own methodology. In his analysis of the flagellum, for example, Dembski does not follow steps 1 through 7 of his own chance-elimination argument. He simply asserts that the flagellum is "specified" without producing either the rejection function or the rejection region his method requires.

5 "Specified complexity" and "complex specified information" are not valid or accepted notions

Dembski's more recent arguments rely, in part, on his self-invented notions of "specified complexity" and "complex specified information" (CSI). These two terms are largely treated as synonyms.

Complexity, in mathematics, physics, and computer science, is a widely-studied notion, and there are many different concepts that fall under the name. Computational complexity, for example, studies the computational resources (such as space and time) required to solve a computational problem [7]. Under this theory, a problem is "complex" if there is no fast algorithm to solve it. Descriptional complexity, on the other hand, assigns a high complexity to a mathematical object (such as a string of symbols) if there is no simple description of it [8]. The most famous example of descriptional complexity is probably Kolmogorov complexity [11]. It is important to note that Dembski's self-invented notion is not any of the mathematically well-recognized definitions of complexity. For example, in his evidence statement, page 3, he states about a sequence of prime numbers, "Because the sequence is long, it is *complex*." (italics in original). On the contrary, according to Kolmogorov complexity, for example, a sequence of prime numbers is *not* complex because it can be generated by a very short algorithm.

Similarly, "information" in mathematics has several well-understood meanings. The most famous, of course, is Shannon information — the basis of information theory — which is a way of measuring uncertainty. Another is the previously-mentioned Kolmogorov complexity, which is sometimes called Kolmogorov information. But Dembski's self-invented "complex specified information" is neither of these measures, either.

Roughly speaking, Dembski says that an event has "specified complexity" if it is of low probability ("complex") and matches an independently-given pattern ("specified"). The lower the probability, the greater the "complexity" in Dembski's sense. There are two significant problems with this definition: Dembski uses an inconsistent methodology for computing these probabilities and his definition of "independently-given" is incoherent.

If a human being is involved in the production of an event, Dembski typically estimates the event's probability relative to an assumption of uniform probability. For example, the probability of a Shakespearean sonnet is evaluated based on a model where each letter is chosen at random. However, if no human being was involved, Dembski usually bases his probability estimate on the causal history of the event in question. This inconsistency means that Dembski can conclude design essentially at whim.

It is also important for Dembski that an observed event match an independently-given

pattern; this is the "specified" portion of specified complexity. In this he is simply following in the footsteps of mathematicians such as Laplace, who argued that random events that match a pattern are less numerous than those that do. However, in order to make this intuition precise, one must explicitly delineate the set of acceptable patterns – something Dembski does not do. The well-accepted theory of Kolmogorov complexity succeeds precisely because legitimate patterns are expressed precisely (as Turing machines) and are measured according to the length of their descriptions. Since Dembski abandons formal description of his patterns, and does not measure their length, nothing in his claims prevents contrived patterns such as "the number of people present at the Last Supper, times the number of moons of Jupiter, plus the code number of secret agent Maxwell Smart" as a description for the integer 437. In this fashion, essentially every event can be "specified". This renders the notion vacuous.

These are some of the reasons that Dembski's notions of "specified complexity" and "complex specified information" are invalid. A more detailed mathematical analysis is given in a longer paper [6].

It is important to note that Dembski's idiosyncratic, self-invented notion of "specified complexity" has not been accepted by the mathematical, statistical, or scientific community. In 2005 I did a search for the term "specified complexity" on the on-line version of *Mathematical Reviews*. I found only two citations for the term, only one of which used it in Dembski's sense - - namely the scathing review of Dembski's book *No Free Lunch* by David Wolpert. I found no citations at all for Dembski's synonym "complex specified information".

This fact has not stopped intelligent design proponents from pretending that "specified complexity" or "complex specified information" are accepted mathematical notions. As an example, consider a 2000 paper by intelligent design proponent Stephen C. Meyer, where he writes, "Systems that are characterized by both specificity and complexity (what information theorists call "specified complexity") have "information content"." [14] I met Meyer at a conference and asked him, What information theorists (plural) use this notion of "specified complexity"? He then admitted that he knew no one but Dembski (who, as I have shown above, has published no papers on information theory).

Neither has Dembski himself been able to apply his notion to anything but toy examples. The example he analyzes again and again is the case of Nicholas Caputo, an official charged with deciding the order of political parties on the election ballot. Caputo, a Democrat, chose the Democrats first in 40 of 41 elections, despite claiming to use a random urn method. Clearly one does not need an extensive methodology to understand why this result suggests fraud.

When it comes to examples where people really do want to know if human design can be inferred — such as distinguishing genuine prehistoric stone artifacts from unworked stone — Dembski is silent, despite being challenged on this point [5].

Dembski has attempted to claim scientific use of his concept of specified complexity by finding other uses of the term in the popular scientific literature. For example, he cites the fact that Paul Davies uses the term in *The Fifth Miracle* and strongly implies that Davies' use of the term is the same as his own. This is simply false. For Davies, the term "complexity" means "high Kolmogorov complexity", whereas for Dembski, complexity is a synonym for improbability.

6 The "Law of Conservation of Information" is not a law

Perhaps the most grandiose of all of Dembski's claims is his so-called "Law of Conservation of Information" (LCI). One version of this "law" is that specified complexity cannot be generated by natural causes. This "law" has simply not been accepted as valid by mathematicians, statisticians, or scientists.

Dembski has claimed that his LCI is compatible with others in the literature. In the context of a discussion on Shannon information, Dembski notes that if an event B is obtained from an event A via a deterministic algorithm, then $P(A\&B) = P(A)$, where P is probability [3, p. 129]. He then goes on to say "This is an instance of what Peter Medawar calls the Law of Conservation of Information" and cites Medawar's book, *The Limits of Science*. Dembski repeats this claim when he discusses his own "Law of Conservation of Information" [3, p. 159]. But Medawar's "law" is not the same as Dembski's.

Medawar was concerned with the amount of information in deductions from axioms in a formal system, as opposed to that in the axioms themselves [13]. He did not formally define exactly what he means by information, but there was no mention of probabilities or the name Shannon. Certainly there is no reason to think that Medawar's "information" has anything to do with Dembski's "complex specified information". Medawar's law, by the way, *can* be made rigorous, but in the context of *Kolmogorov* information, not Shannon information or Dembski's "complex specified information".

In my paper with Elsberry [6], we give several examples of how Dembski's claims about LCI are flawed. For example, here is how applying a function may indeed increase "specified complexity":

Suppose j is an English message of 1000 characters (English messages apparently always being specified), $f(i) = j$, and f is a mysterious decryption function which is unknown to the intelligent agent A who identified j as CSI. Perhaps f is computed by a "black box" whose workings are unknown to A, or perhaps A simply stumbles along j which was produced by f at some time in the distant past. The intelligent agent A who can identify j as CSI will be unable, given an occurrence of i, to identify *it* as CSI, since f is unknown to A. Thus, in A's view, CSI j was actually *produced* by applying f to i. The only way out of this paradox is to *change* A's background knowledge to include knowledge about f. But then Dembski's claim about conservation of CSI is falsified, since it no longer applies to all functions, but only functions specifiable through A's background knowledge K.

This error becomes even more important when j arises through a very long causal history, where thousands or millions of functions have been applied to produce j. It is clearly unreasonable to assume that both the initial probability distribution, which may depend on initial conditions billions of years in the past, *and* the complete causal history of transformations, be known to an intelligent agent reasoning about j.[3] But it is *crucial* that every single step be known; the omission of a *single* transformation by a function f has the potential to skew the estimated probabilities in such a way that LCI no longer holds.

[3]Dembski seems to admit this when he says that "...most claims are like this (i.e., they fail to induce well-defined probability distributions)..." [3, p. 106].

7 Conclusions

William Dembski has not made a significant contribution to a mathematical or scientific understanding of "design". His work is not regarded as significant by information theorists, mathematicians, statisticians, or computer scientists. He does not present his work in the generally-accepted fora for results in these fields. His mathematical work is riddled with errors and inconsistencies that he has not acknowledged. The word "pseudomathematics" is appropriate to describe his work.

References

[1] Tony Carnes, "Design Interference", *Christianity Today*, December 4, 2000. Available at http://www.christianitytoday.com/ct/2000/014/18.20.html.

[2] W. A. Dembski. *Intelligent Design: The Bridge Between Science & Theology.* InterVarsity Press, 1999.

[3] W. A. Dembski. *No Free Lunch: Why Specified Complexity Cannot Be Purchased Without Intelligence.* Rowman & Littlefield, 2002.

[4] "A Scientific Dissent from Darwinism", http://www.discovery.org/articleFiles/PDFs/100ScientistsAd.pdf

[5] Wesley Elsberry and Jeffrey Shallit, Eight challenges for intelligent design advocates, *Reports of the NCSE* 23 No. 5-6, (Sept.-Dec. 2003), 23–25.

[6] Wesley Elsberry and Jeffrey Shallit, Information theory, evolutionary computation, and Dembski's complex specified information, submitted. A previous version is available at http://www.talkreason.org/articles/eandsdembski.pdf.

[7] Michael R. Garey and David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman, 1979.

[8] Jonathan Goldstine, Martin Kappes, Chandra M. R. Kintala, Hing Leung, Andreas Malcher, and Detlef Wotschke, Descriptional Complexity of Machines with Limited Resources, *J. Universal Comput. Sci.* 8 (2002) (2), 193–234.

[9] A. Hewish, S. J. Bell, J. D. H. Pilkington, P. F. Scott, and R. A. Collins. Observation of a rapidly pulsating radio source. *Nature* **217** (February 24, 1968), 709–713.

[10] M. A. Kessler and B. T. Werner, Self-organization of sorted patterned ground, *Science* **299** (2003), 380–383.

[11] M. Li and P. Vit''anyi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer, 1997.

[12] Beth McMurtrie, "Darwinism Under Attack", *Chronicle of Higher Education*, December 21, 2001. Available at http://chronicle.com/free/v48/i17/17a00801.htm.

[13] P. B. Medawar. *The Limits of Science*. Harper & Row, 1984.

[14] S. C. Meyer. DNA and other designs. *First Things* , No. 102, (April 2000), 30–38.

[15] Jason Rosenhouse, *Probability, optimization, and evolution*, *Evolution* 56 (8), 2002, 1721–1722.

[16] Jeffrey Shallit, Book review of *No Free Lunch*, *BioSystems* 66 (2002), 93–99.

[17] Jeffrey Shallit, The story of an ID urban legend, *Reports of the NCSE* 23 No. 5-6, (Sept-Dec. 2003), 39.

[18] Jeffrey Shallit, Dembski's mathematical achievements, `http://www.pandasthumb.org/pt-archives/000207.html`.

[19] Jeffrey Shallit and Wesley Elsberry, "Playing games with probability: Dembski's complex specified information", in Matt Young and Taner Edis, eds., *Why Intelligent Design Fails: A Scientific Critique of the New Creationism*, Rutgers University Press, 2004, pp. 121–138.

[20] Karl Sims, "Evolving 3D morphology and behavior by competition". In R. A. Brooks and P. Maes, eds., *Artificial Life IV: Proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems*, MIT Press, 1994, pp. 28–39.

[21] `http://www.pandasthumb.org/pt-archives/000130.html` .

A Appendix: Curriculum Vitae of Jeffrey Shallit

Jeffrey Shallit
Professor and Director of Graduate Studies
School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1
(519) 888-4804
(519) 885-1208 (fax)
E-Mail: shallit@graceland.uwaterloo.ca

Home Page: http://www.cs.uwaterloo.ca/~shallit

Citizenship: U. S. (Canadian permanent resident)

Education

Ph.D., Mathematics, University of California, Berkeley, June 1983.
Advisor: David Goldschmidt (de jure); Manuel Blum (de facto).
Dissertation: *Metric Theory of Pierce Expansions.*

A.B., Mathematics, Princeton University, June 1979, *cum laude.*
Thesis: *Integer Functions and Continued Fractions.*

Awards

University of Waterloo Mathematics Faculty Fellowship May 1 2004 – April 30 2007.

Employment

July 2000 – date, Full Professor, Department of Computer Science, University of Waterloo.

September 1990 – date, Associate Professor (tenured), Department of Computer Science, University of Waterloo.

September 1989 – December 1989, Visiting Assistant Professor, University of Wisconsin, Madison (on leave from Dartmouth).

July 1988 – September 1990: Assistant Professor, Department of Mathematics and Computer Science, Dartmouth College.

September 1985 – November 1985, Professeur Associé, Département de Mathématiques et Informatique, Université de Bordeaux I (on leave from Chicago).

September, 1983 – June, 1988: Assistant Professor, Department of Computer Science, University of Chicago.

September 1984: Summer Research Faculty, IBM Yorktown Heights.

September, 1979 – August, 1983 (part-time while at Berkeley): Programmer, Computing Services, University of California, Berkeley.

September, 1975 – August, 1979 (part-time while at Princeton): Consultant, Computer Center, Princeton University, Princeton, NJ.

1974 – 1977 (part-time): APL Programmer, The Yardley Group, Philadelphia, PA.

Areas of interest

Formal languages, combinatorics on words, automata theory, complexity theory, number theory, algorithmic number theory, combinatorics, algebra, ethical use of computers, history of mathematics and computer science, pseudoscience, pseudomathematics.

Publications

Co-authors who were my graduate students at the time are marked with an asterisk.

Articles in Refereed Journals

1. "A simple proof that phi is irrational", *Fib. Quart.*, **13** (1975), 32.

2. "An interesting continued fraction", *Math. Mag.*, **48** (1975), 207–211.

3. "Predictable regular continued cotangent expansions", *J. Res. Nat. Bur. Standards - B. Math. Sciences*, **80B** (1976), 285–290.

4. (with David Rosen), "A continued fraction algorithm for approximating all real polynomial roots", *Math. Mag.* **51** (1978), 112–116.

5. "Simple continued fractions for some irrational numbers", *J. Number Theory* **11** (1979), 209–217.

6. "Explicit descriptions of some continued fractions", *Fib. Quart.* **20** (1982), 77–81.

7. "Simple continued fractions for some irrational numbers II", *J. Number Theory*, **14** (1982), 228–231.

8. (with John Hughes) "On the number of multiplicative partitions", *Am. Math. Monthly* **90** (1983), 468–471.

9. "Some predictable Pierce expansions", *Fib. Quart.* **22** (1984), 332–335.

10. (with Jon Yamron), "On linear recurrences and divisibility by primes", *Fib. Quart.* **22** (1984), 366–368.

11. (with Adi Shamir), "Number-theoretic functions which are equivalent to number of divisors", *Info. Proc. Letters* **20** (1985), 151–153.

12. "On infinite products associated with sums of digits", *J. Number Theory* **21** (1985), 128–134.

13. (with Eric Bach and Gary Miller), "Sums of divisors, perfect numbers, and factoring", *SIAM J. Comput.* **15** (1986), 1143–1154.

14. "Metric theory of Pierce expansions", *Fib. Quart.* **24** (1986), 22–40.

15. (with Michael Rabin) "Randomized algorithms in number theory", *Commun. Pure and Appl. Math.* **39** (1986), S239–S256.

16. (with Jean-Paul Allouche, Henri Cohen, and Michel Mendès France) "De nouveaux curieux produits infinis", *Acta Arithmetica* **49** (1987), 141–153.

17. "A generalization of automatic sequences", *Theor. Comput. Sci.* **61** (1988) 1–16.

18. (with David Rubinstein and Mario Szegedy), "A subset-coloring algorithm and its applications to computer graphics", *Commun. ACM* **31** (1988), 1228–1232.

19. (with Jean-Paul Allouche), "Infinite products associated with counting blocks in binary strings", *J. London Math. Soc.*, **39** (1989), 193–204.

20. (with Eric Bach), "Factoring with cyclotomic polynomials", *Mathematics of Computation* **52** (1989), 201–219.

21. (with Jean-Paul Allouche and Peter Hajnal), "Analysis of an infinite product algorithm", *SIAM J. on Discrete Math.* **2** (1989), 1–15.

22. (with Michel Mendès France) "Wire-bending", *J. Combinatorial Theory (Series A)*, **50** (1989), 1–23.

23. (with Jean-Paul Allouche and J. Betrema), "Sur des points fixes de morphismes du monoide libre", *RAIRO Informatique* **23** (1989), 235–249.

24. (with Jorge Stolfi), "Two methods for the generation of fractal images", *Computers and Graphics* 13 (1989), 185–191.

25. "On the worst case of three algorithms for computing the Jacobi symbol", *J. Symbolic Computation* **10** (1990), 593–610.

26. (with J. L. Davison), "Continued fractions for some alternating series", *Monatshefte Math.* **111** (1991), 119–126.

27. (with P. Erdös), "New bounds on the length of finite Pierce and Engel series", *Séminaire de Théorie des Nombres de Bordeaux* **3** (1991), 43–53.

28. (with J.-P. Allouche and P. Morton) "Pattern spectra, substring enumeration, and automatic sequences", *Theor. Comput. Sci.* **94** (1992), 161–174.

29. (with J.-P. Allouche) "The ring of k-regular sequences", *Theor. Comput. Sci.* **98** (1992), 163–197.

30. (with A. J. van der Poorten) "Folded continued fractions", *J. Number Theory* **40** (1992), 237–250.

31. "Real numbers with bounded partial quotients: a survey", *L'Enseignement Math.* **38** (1992), 151–187.

32. (with Eric Bach and James Driscoll) "Factor refinement", *J. Algorithms* **15** (1993), 199–222.

33. (with A. J. van der Poorten), "A specialised continued fraction", *Canad. J. Math.* **45** (1993), 1067–1079.

34. (with J.-P. Allouche), "Complexité des suites de Rudin-Shapiro généralisées", *Journal de Théorie des Nombres de Bordeaux* 5 (1993), 283–302.

35. "On the maximum number of distinct factors in a binary string", *Graphs and Combinatorics* **9** (1993), 197–200.

36. (with H. W. Lenstra, Jr.) "Continued fractions and linear recurrences", *Math. Comp.* **61** (1993), 351–354.

37. "Rational numbers with non-terminating, non-periodic modified Engel-type expansions", *Fibonacci Quarterly* **31** (1993), 37–40.

38. (with P. Enflo, A. Granville, and S. Yu) "On sparse languages L such that $LL = \Sigma^*$", *Discrete Applied Mathematics* **52** (1994), 275–285.

39. "Numeration systems, linear recurrences, and regular sets", *Information and Computation* **113** (1994), 331–347.

40. "Pierce expansions and rules for the determination of leap years", *Fibonacci Quart.* **32** (1994), 416–423.

41. (with J.-P. Allouche, D. Astoorian, and J. Randall), "Morphisms, squarefree strings, and the Tower of Hanoi puzzle", *Amer. Math. Monthly* **101** (1994), 651–658.

42. (with J. Sorenson), "Analysis of a left-shift binary GCD algorithm", *J. Symbolic Computation*, **17** (1994), 473–486.

43. "Origins of the analysis of the Euclidean algorithm", *Historia Mathematica*, **21** (1994), 401–419.

44. (with J. Tromp), "Subword complexity of a generalized Thue-Morse word", *Information Processing Letters* **54** (1995), 313–316.

45. (with J.-P. Allouche, E. Cateland, H.-O. Peitgen, and G. Skordev) "Automatic maps on a semiring with digits", *Fractals* **3** (1995), 663–677.

46. (with F. Morain and H. C. Williams), "Discovery of a lost factoring machine", *Math. Intelligencer* **17** (3) (Summer 1995), 41–47.

47. (with Y. Breitbart), "Automaticity I: Properties of a measure of descriptional complexity", *J. Comput. System Sci.* **53** (1996), 10–25.

48. (with J.-P. Allouche, A. Lubiw, M. Mendès France, and A. van der Poorten) "Convergents of folded continued fractions", *Acta Arithmetica* **77** (1996), 77–96.

49. (with E. Bach, R. Lukes, and H. C. Williams), "Some results and estimates on pseudopowers", *Math. Comp.* **65** (1996), 1737–1747.

50. (with S. Lehr and J. Tromp), "On the vector space of the automatic reals" *Theoret. Comput. Sci.*, **163** (1996), 193–210.

51. (with I. Glaister*), "A lower bound technique for the size of nondeterministic finite automata", *Information Processing Letters* **59** (1996), 75–77.

52. (with F. Morain and H. C. Williams), "La machine à congruences", *La Revue, Musée des Arts et Métiers (Paris)*, **14** (March 1996), 14–19.

53. "Automaticity IV: Sequences, Sets, and Diversity", *Journal de Théorie des Nombres de Bordeaux* **8** (1996), 347–367.

54. (with C. Pomerance and J. Robson), "Automaticity II: Descriptional complexity in the unary case", *Theoret. Comput. Sci.* **180** (1997), 181–201.

55. (with J.-P. Allouche, E. Cateland, W. J. Gilbert, H.-O. Peitgen, and G. Skordev), "Automatic maps in exotic numeration systems" *Theory Comput. Syst.* **30** (1997), 285–331.

56. (with J. C. Lagarias), "Linear fractional transformations of continued fractions with bounded partial quotients", *J. Théorie Nombres Bordeaux* **9** (1997), 267–279.

57. (with Harriet Lyons), "Social issues of networking in Canada's information society", *The Information Society* **13** (1997), 147–151.

58. (with I. Glaister*), "Automaticity III: Polynomial automaticity and context-free languages", *Computational Complexity* **7** (1998), 371–387.

59. (with Jean-Paul Allouche and James Currie), "Extremal infinite overlap-free binary words", *Electronic J. Combinatorics*, **5** (1) (1998), #R27.

60. (with Ming-wei Wang*), "On minimal words with given subword complexity", *Electronic J. Combinatorics* **5** (1) (1998), #R35.

61. (with Jean-Paul Allouche), "Generalized perturbed symmetry", *European J. Combinatorics* **19** (1998), 401–411.

62. (with Ming-wei Wang*), "An inequality for non-negative matrices", *Linear Algebra and Its Applications* **290** (1999), 135–144.

63. (with J. F. Buss and G. S. Frandsen), "The computational complexity of some problems of linear algebra", *J. Comput. System Sci.* **58** (1999), 572–596.

64. (with J. Currie, H. Petersen, and J. M. Robson), "Separating words with small grammars", *J. Automata, Languages, and Combinatorics* **4** (1999), 101–110.

65. "Automaticity and Rationality", *J. Automata, Languages, and Combinatorics* **5** (2000), 255–268.

66. (with Jean-Paul Allouche) "Sums of digits, overlaps, and palindromes", *Discrete Math. and Theoretical Computer Science*, 4 (2000), 1–10.

67. (with G. Boros and V. Moll), "The 2-adic valuation of the coefficients of a polynomial, *Scientia Ser. A* 7 (2000-1), 47-60.

68. (with G. Pighizzini), "Unary language operations, state complexity, and Jacobsthal's function", *Int'l. J. Found. Comput. Sci.* **13** (2002), 145–159.

69. (with J. Ellis and H. Fan), "The cycles of the multiway perfect shuffle permutation", *Discrete Mathematics & Theoretical Computer Science* 5 (2002), 169–180.

70. (with Ming-wei Wang*), "On two-sided infinite fixed points of morphisms", *Theoret. Comput. Sci.* **270** (2002), 659–675.

71. (with Ming-wei Wang*), "Automatic complexity of strings", *J. Autom. Lang. Comb.* **6** (2001), 537–554.

72. (with S. Cautis, F. Mignosi, M.-w. Wang*, S. Yazdani), "Periodicity, morphisms, and matrices", *Theoret. Comput. Sci.* **295** (2003), 107-121.

73. (with M. Domaratzki and G. Pighizzini), "Simulating finite automata with context-free grammars", *Info. Proc. Letters* **84** (2002), 339–344.

74. (with G. Pighizzini and M.-w. Wang*), "Unary context-free grammars and pushdown automata, descriptional complexity, and auxiliary space lower bounds", *J. Comput. System Sci.* **65** (2002), 393–414.

75. (with M. Domaratzki, D. Kisman) On the number of distinct languages accepted by finite automata with n states, *J. Autom. Lang. Comb.* **7** (2002), 469–486.

76. What this country needs is an 18-cent piece, *Math. Intelligencer* **25** (2) (2003), 20-23.

77. (with Jean-Paul Allouche), The ring of k-regular sequences, II, *Theoret. Comput. Sci.* **307** (2003), 3-29.

78. (with S. Cautis, F. Mignosi, M.-w. Wang*, and S. Yazdani), Periodicity, morphisms, and matrices, *Theor. Comput. Sci.* **295** (2003), 107–121.

79. (with Troy Vasiga*), On the iteration of certain quadratic maps over $GF(p)$, *Discrete Math.* **277** (2004), 219–240.

80. The mathematics of Per Nørgård's rhythmic infinity system, to appear, *Fibonacci Quarterly*.

81. (with J. Karhumäki) Polynomial versus exponential growth in repetition-free binary words, *J. Combinatorial Theory Ser. A* **105** (2004), 335-347.

82. Simultaneous avoidance of large squares and fractional powers in infinite binary words, *Int'l. J. Found. Comput. Sci.* 15 (2004), 317–327.

83. (with J.-P. Allouche and G. Skordev), "Self-generating sets, integers with missing blocks, and substitutions", to appear, *Discrete Mathematics*.

Articles Submitted

1. (with W. Elsberry), "Information theory, evolutionary computation, and Dembski's "complex specified information", submitted.

2. (with M. Domaratzki and A. Okhotin), Enumeration of context-free languages, submitted.

Articles in Refereed Conference Proceedings

1. (with Eugene McDonnell), "Extending APL to infinity", *Proc. APL 80 Int'l Conf.* North-Holland, Amsterdam, 1980, pp. 123–132.

2. "Infinite arrays and diagonalization", Proc. APL 81 Conf., *APL Quote-Quad* **12** (1) (September 1981), 281–285.

3. "Computational simplicial homology in APL", APL 82 Conf. Proc., *APL Quote Quad* **13** (1) (September 1982), 332–338.

4. "Merrily we roll along: some aspects of ?", APL 83 Conf. Proc., *APL Quote Quad*, **13** (3) (March 1983), 243–249.

5. (with Eric Bach and Gary Miller), "Sums of divisors, perfect numbers, and factoring", *16th ACM Symp. Theor. Comput.* (1984), 183–190.

6. (with Eric Bach), "Factoring with cyclotomic polynomials", *26th Symposium on Foundations of Computer Science* (1985), 443–450.

7. "A generalization of automatic sequences", *STACS '89*, B. Monien and R. Cori, eds., Lecture Notes in Computer Science **349**, 156–167.

8. (with Jean-Paul Allouche), "Sums of digits and the Hurwitz zeta function", in K. Nagasaka and E. Fouvry, eds., *Analytic Number Theory: Proc. Japanese-French Symposium Held in Tokyo, Japan, October 10-13, 1988*, Lecture Notes in Mathematics #1434, Springer-Verlag, 1990, pp. 19–30.

9. (with Eric Bach and James Driscoll), "Factor refinement", *Proc. First Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 1990, pp. 201–211.

10. (with J.-P. Allouche), "The ring of k-regular sequences", Proceedings of STACS 1990, Lecture Notes in Computer Science #415, pp. 12–23.

11. "Numeration systems, linear recurrences, and regular sets", *Automata, Languages, and Programming: 19th International Colloquium*, W. Kuich, ed., Lecture Notes in Computer Science, vol. 623, Springer-Verlag, 1992, pp. 89–100.

12. (with A. Szilard, S. Yu, and K. Zhang), "Characterizing regular languages with polynomial densities", *Proc. 17th Int'l Symp. Math. Found. Comp. Sci. (MFCS)*, I. M. Havel and V. Koubek, eds., Lecture Notes in Computer Science, vol. 629, 1992, pp. 494–503.

13. (with Y. Breitbart), "Automaticity I: Properties of a measure of descriptional complexity", *STACS '94: 11th Annual Symposium on Theoretical Aspects of Computer Science*, P. Enjalbert et al., eds., Lecture Notes in Computer Science vol. 775, 1994, pp. 619–630.

14. (with S. Lehr and J. Tromp), "On the vector space of the automatic reals", in *Formal Power Series and Algebraic Combinatorics*, 7th Conference, 1995, pp. 351–362.

15. (with I. Glaister*), "Polynomial automaticity, context-free languages, and fixed points of morphisms", in W. Penczek and A. Szalas, eds., *Mathematical Foundations of Computer Science (MFCS '96)*, Lecture Notes in Computer Science #1113, Springer, 1996, pp. 382–393.

16. (with J. F. Buss and G. S. Frandsen), "The computational complexity of some problems of linear algebra", in R. Reischuk and M. Morvan, eds., *STACS 97: 14th Annual Symposium on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science #1200, Springer-Verlag, 1997, pp. 451–462.

17. (with M. Mendès France and A. J. van der Poorten), "On lacunary formal power series and their continued fraction expansion", in K. Győry, H. Iwaniec, and J. Urbanowicz, eds., *Number Theory in Progress*, Walter de Gruyter, 1999, 321–326.

18. (with C. Lam and S. Vanstone), "Worst-case analysis of an algorithm for computing the greatest common divisor of n inputs", in J. Buchmann, T. Høholdt, H. Stichtenoth, and H. Tapia-Recillas, eds., *Coding Theory, Cryptography and Related Areas*, Springer-Verlag, 2000, pp. 156–166.

19. (with J.-P. Allouche), "The ubiquitous Prouhet-Thue-Morse sequence", in C. Ding, T. Helleseth, and H. Niederreiter, eds., *Sequences and their Applications: Proceedings of SETA '98*, Springer, 1999, pp. 1–16.

20. (with D. Swart*), "An efficient algorithm for computing the i'th letter of $\varphi^n(a)$", Proc. 10th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 1999, pp. 768–775.

21. (with J. Loftus* and Ming-wei Wang*), "New problems of pattern avoidance", in G. Rozenberg and W. Thomas, eds., *Developments in Language Theory* (DLT '99), World Scientific Press, pp. 185–199.

22. (with Ming-wei Wang*), "On two-sided infinite fixed points of morphisms", in G. Ciobanu and G. Păun, eds., *Proc. 12th Int'l. Symp. Fundamentals of Computation Theory (FCT '99)*, 1999, Lecture Notes in Computer Science #1684, pp. 488–499.

23. "State complexity and Jacobsthal's function", in S. Yu and A. Păun, eds., *Implementation and Application of Automata, Proc. 5th CIAA*, 2000, Lecture Notes in Computer Science #2088, pp. 272–278.

24. (with F. Mignosi and M.-w. Wang*), "Variations on a theorem of Fine & Wilf", in J. Sgall, A. Pultr, and P. Kolman, eds., *Proc. 26th Mathematical Foundations of Computer Science (MFCS 2001)*, 2001, Lecture Notes in Computer Science # 2136, pp. 512–523.

25. (with M. Domaratzki* and S. Yu), "Minimal covers of formal languages", in W. Kuich, G. Rozenberg, and A. Salomaa, *Proc. 5th Developments in Language Theory (DLT 2001)*, 2001, Lecture Notes in Computer Science # 2295, pp. 319–329.

26. (with K. Ellul* and M.-w. Wang*), "Regular expressions: new results and open problems", in Pre-Proceedings of Descriptional Complexity of Formal Systems (DCFS), 2002, pp. 17–34.

27. (with J. Lee), "Enumerating regular expressions and their languages", to appear, *Proc. of CIAA 2004*, LNCS 3314, 2005, pages 2–22.

Chapters in Books

1. "A triangle for the Bell numbers", in Verner E. Hoggatt, Jr. and Marjorie Bicknell-Johnson, eds., *A Collection of Manuscripts Related to the Fibonacci Sequence*, Fibonacci Association, Santa Clara, Ca. 1980, pp. 69–71.

2. (with Michel Mendès France) "Wire-bending", In Humiaki Huzita, ed., *Proc. 1st International Meeting of Origami Science and Technology*, Ferrara, Italy, Dec. 6–7, 1989, pp. 295–317.

3. (with H. C. Williams), "Computational number theory before computers", in Walter Gautschi, ed., *Mathematics of Computation 1943–1993: A Half-Century of Computational Mathematics*, *Proc. Symp. Appl. Math.* 48 (1994), 481–531.

4. "Public networks and censorship", in Peter Ludlow, ed., *High Noon on the Electronic Frontier*, MIT Press, 1996, pp. 275–289.

5. "Number theory and formal languages", in D. A. Hejhal, J. Friedman, M. C. Gutzwiller, and A. M. Odlyzko, eds., *Emerging Applications of Number Theory*, IMA Volumes in Mathematics and Its Applications, V. 109, 1999, pp. 547–570.

6. "Ten fallacies of Internet censorship", in B. Szuchewycz and J. Sloniowski, eds., *Canadian Communications: Issues in Contemporary Media and Culture*, Prentice Hall Allyn and Bacon Canada, 1999, pp. 427–431.

7. "Diophantine approximation", in *CRC Handbook of Discrete and Combinatorial Mathematics*, K. Rosen, ed., 1999, pp. 289–294.

8. "The fallacies of Internet censorship", in Lester Faigley and Jack Selzer, eds., *Good Reasons with Contemporary Arguments*, Allyn and Bacon, 2001, pp. 552-561.

9. Formal languages and number theory, in M. B. Nathanson, ed., *Unusual Applications of Number Theory*, Proc. DIMACS Workshop January 10–14, 2000, American Mathematical Society, 2004, pp. 169–181.

10. (with W. Elsberry) "Playing Games with Probability: Dembski's Complex Specified Information", in *Why Intelligent Design Fails: A Scientific Critique of the New Creationism*, Rutgers University Press, 2004, pp. 121–138.

Books

1. (with Eric Bach) *Algorithmic Number Theory*, Vol. 1: Efficient Algorithms, MIT Press, 1996.

2. (with Jean-Paul Allouche), *Formal Languages and Number Theory*, 571 pp., Cambridge University Press, 2003.

3. *Advanced Topics in Formal Languages and Automata Theory*, accepted for publication, Cambridge University Press.

Other Publications

1. "Calculation of $\sqrt{5}$ and ϕ to 10,000 decimal places", reviewed in *Math. Comp.* **30** (1976), 377.

2. "The prime factorization of 1", *APL Quote Quad* **6** (4) (Winter 1976), 36–37.

3. "Table of Bell numbers to B(400)", reviewed in *Math. Comp.* **32** (1978), 656.

4. "Resolution of algebraic rational functions into partial fractions", Algorithm 140, *APL Quote-Quad*, **10** (3) (March 1980), 28–29.

5. "V-partitions and permutations by inversions", *APL Quote Quad* **12** (3) (March 1982), 15–17.

6. "Discriminant of a polynomial in one variable over the integers", *APL Quote Quad* **12** (4) (June 1982), 11–12.

7. "A simple proof of the Lucas-Lehmer primality test", Univ. of Chicago Department of Computer Science, Technical Report 84–002, April 1984.

8. "An application of the Lenstra-Lenstra-Lovász algorithm to the solution of a Diophantine equation", Univ. of Chicago, Department of Computer Science, Technical Report 84-003, May 1984.
9. "An exposition of Pollard's algorithm for quadratic congruences", University of Chicago Technical Report 84–006, December, 1984.
10. (with Eric Bach) "A class of functions equivalent to factoring", University of Chicago Technical Report 84–008, December, 1984.
11. "Random polynomial time algorithms for sums of squares", University of Chicago Technical Report 85–001, January, 1985.
12. "Sur certains produits infinis liés aux sommes des chiffres", Groupe d'étude en théorie analytique des nombres, Institut Henri Poincaré, Paris, 3e année, 1985/6, 3.01–3.05.
13. "Sur la complexité de fonctions arithmétiques", Seminaire de Théorie des Nombres, Université de Bordeaux I, 1985–6, 1.01–1.06.
14. "Automates finis, pliage de fil de fer, et fractions continues", *Séminaire de théorie des nombres de Bordeaux*, 1986–7, pp. 1–13.
15. "Appendix to the paper of Salon", *Séminaire de théorie des nombres de Bordeaux*, 1986–7, Exposé 4, 4.29.A-4.36.A.
16. "Fractals, bitmaps, and APL", *APL Quote-Quad* 18 (3) (March 1988), 24–32.
17. "A note on the relative complexity of $\sigma_k(N)$ and $d(N)$", University of Chicago, Department of Computer Science, Technical Report 88-001, January 1988.
18. "Some facts about continued fractions that should be better known", University of Waterloo, Computer Science Department, Research Report CS–91–30, July 1991.
19. "Description of generalized continued fractions by finite automata", University of Waterloo, Computer Science Department, Research Report CS 91–44, September 1991.
20. "Characteristic words as fixed points of homomorphisms", University of Waterloo, Computer Science Department, Research Report CS–91–72, December 1991.
21. (with D. Wilson), The "$3x + 1$" problem and finite automata, *Bulletin of the EATCS*, No. 46 (February 1992), 182–185.
22. (with J. Sorenson), "A binary algorithm for the Jacobi symbol", *ACM SIGSAM Bulletin*, 27 (1) (January 1993), 4–11.
23. "Should governments try to censor the Internet?", *The Costco Connection*, 10 (3), May/June 1997, p. 14.
24. "Minimal primes", *J. Recreational Mathematics* 30 (2) (1999-2000), 113–117.

25. (with David Hamm*), "Characterization of finite and one-sided infinite fixed points of morphisms on free monoids", University of Waterloo Technical Report CS-99-17, July 1999.

26. "The computational complexity of the local postage stamp problem", *SIGACT News* 33 (1) (March 2002), 90–94.

Book Reviews

1. Book review of Paul Gross and Norman Levitt, *Higher Superstition*, in *Skeptic* 3 (1) (1994), 98–100.

2. Book Review of Cavazos & Morin, *Cyberspace and the Law: Your Rights and Duties in the On-Line World*, in John J. Makay, Editor, *Free Speech Yearbook*, 33 (1995), 179–181 (Southern Illinois University Press, Carbondale, IL).

3. Book review of Menezes, van Oorschot, and Vanstone, *Handbook of Applied Cryptography*, and Rosenheim, *The Cryptographic Imagination: Secret Writings from Edgar Poe to the Internet*, in *Amer. Math. Monthly* 106 (1999), 80–83.

4. Book review of Patrick Glynn, *God: The Evidence*, in *Skeptic* 6 (2) (1998), 80–82.

5. Book review of William Dembski, *No Free Lunch*, in *BioSystems* 66 (2002), 93–99.

Invited Addresses

January, 1992: "Real numbers with bounded partial quotients", MAA Invited Lecture, Annual Joint Meeting of AMS/MAA, Baltimore, Maryland.

July, 1994: "Old and New Results on Continued Fractions", Canadian Number Theory Association, CNTA'94, Halifax, Nova Scotia.

January, 1995: "Public Networks and Censorship", Ontario Library Association, Toronto, Ontario.

December, 1995: "Remarks on Inferring Integer Sequences", Canadian Mathematical Association, Vancouver, BC.

May 1996, invited speaker, "The real meaning of free speech in cyberspace", at the conference "The Internet: Beyond the Year 2000", University of Toronto.

July 1996, Plenary Speaker, "Automaticity", Conference on Emerging Applications of Number Theory, Institute of Mathematics and Its Applications, Minneapolis, MN.

December 1996, 19th Annual Alexander Graham Bell Lecture at McMaster University (debate with C. C. Gotlieb).

June, 1997: "Number Theory and Formal Languages", Number Theory Day, University of the Witwatersrand, Johannesburg, South Africa.

July, 1999: "Automaticity", Descriptional Complexity of Automata, Grammars, and Related Structures, Magdeburg, Germany.

March, 2000: Invited speaker at 3rd International Colloquium on Words, Languages, and Combinatorics, Kyoto, Japan.

August 2002: Invited speaker at Descriptional Complexity of Formal Systems, London, Ontario.

July 2004, Invited speaker at CIAA (Conference on Implementation and Application of Automata) 2004, Kingston, Ontario.

Grant Record

NSERC Canada, Research Grant, CDN $ 43,000/yr. April 2003 - March 2008.

NSERC Canada, Individual Operating Grant, CDN $29,000/yr., April 1998 – March 2003.

NSERC - CRD, CDN $81,120 in 1994; $224,894 in 1995 - 1997, (co-held with K. Geddes and two others).

ITRC, CDN $63,500/yr., 1993–1995, (co-held with K. Geddes and four others).

NSERC Canada, Individual Operating Grant, CDN $26,000/yr., April 1994 – March 1998.

ITRC, Research Award, CDN $20,000/yr., April 1993 – March 1994 (co-held with Ming Li).

ITRC, Research Award, CDN $60,000/yr., April 1991 - March 1993 (co-held with Keith Geddes and George Labahn).

NSERC Equipment Award, CDN $67,601, April 1992 – March 1993, (co-held with Keith Geddes and five others).

ITRC, Research Award, CDN $30,000/yr., April 1991 – March 1993, (co-held with Prabhakar Ragde and many others).

NSERC Canada, Individual Operating Grant, CDN $24,000/yr., April 1991 - March 1994.

University of Waterloo Interim Grant, September 1990, CDN $4,000.

Wisconsin Alumni Research Fund, University of Wisconsin, September 1989, US $5,750.

Walter Burke Award, Dartmouth College, November 1988, US $15,000.

National Science Foundation Grant, September 1988 - August 1990, US $49,653.

Research appointment, CNRS (French National Science Foundation), Fall 1986, US $12,000.

Ph.D. Students

1. Ming-wei Wang, began May 1999, finished 2004.
2. Troy Vasiga, began January 2000.
3. Narad Rampersad, began Fall 2004.
4. Dalia Krieger, began Fall 2004.

M. Math. Students

1. Michael Domaratzki, M. Math. student, 2001.

2. Ming-wei Wang, M. Math., thesis option, 1999. *Subword complexity and a matrix inequality.*

3. David Swart, M. Math., thesis option, 1998. *Calculating the ith letter of the nth word in a DOL-sequence.*

4. David Hamm, M. Math., thesis option, 1998. *Contributions to Formal Language Theory: Fixed Points, Complexity, and Context-Free Sequences.*

5. Ian Matthew Glaister, M. Math., thesis option, 1995. *Automaticity and Closure Properties.*

6. Qi Xiang Zhang, M. Math., essay option, 1994.

7. Peter Wei Liang Liu, M. Math., essay option, 1994.

Society Memberships

American Mathematical Society
Association for Computing Machinery
Canadian Mathematical Society
Electronic Frontier Foundation
European Association for Theoretical Computer Science

Editorial Positions

Editorial Board, *Journal de Théorie des Nombres de Bordeaux*, 1991–date
Editorial Board, *Journal of Integer Sequences* (electronic), 1998–date
Collaborating Editor, *American Mathematical Monthly*, Problem Section, 1983–1996.

Conference Organization

Co-organizer, *Free Speech and Privacy in the Information Age* University of Waterloo, November 1994.

Co-organizer, Special Session on Automatic Sequences and Related Topics, Canadian Mathematical Society, Summer Meeting, 2005.

Program Committee Member:
Latin American Conference on Theoretical Informatics (LATIN '92)
ISSAC 94
International Conference on Sequences and Their Applications (SETA '98)
Descriptional Complexity of Automata, Grammars, and Related Structures (DCAGRS 2000)

Refereeing and Reviewing for Journals

1. Reviewer, Mathematical Reviews (approximately 5 reviews/yr.)

2. Referee (approx. 6-10 articles refereed per year)

International Journal of Algebra and Computation
Information Processing Letters
Mathematics of Computation
Discrete Mathematics
Journal of the Australian Mathematical Society
Journal of the American Mathematical Society
Proceedings of the American Mathematical Society
Theoretical Computer Science
IEEE Transactions on Information Theory
Mathematical Reviews
Journal of Number Theory
American Mathematical Monthly
SIAM Journal on Computing
Utilitas Mathematica
Pattern Recognition Letters
Fibonacci Quarterly
Canadian Mathematical Bulletin
Algebra Colloquium
The Information Society
Designs, Codes, and Cryptography
Theory of Computing Systems
Experimental Mathematics
College Mathematics Journal